

# PERSPECTIVES INTERNATIONALES

Cadre de référence IIA pour l'audit de l'intelligence artificielle

Applications pratiques, Partie A

*Édition spéciale*



## Table des matières

Introduction .....	2
Le Cadre de référence IIA pour l'audit de l'intelligence artificielle ...	2
Stratégie relative à l'intelligence artificielle .....	3
Cyber résilience .....	3
Compétences en intelligence artificielle .....	4
Gouvernance .....	5
Obligation de rendre compte, responsabilité et supervision .	6
Régulateurs .....	6
Organe de gouvernance / Conseil / Comité d'audit ....	7
Direction générale .....	7
Première ligne de maîtrise .....	7
Deuxième ligne de maîtrise .....	7
Troisième ligne de maîtrise .....	7
Audit externe .....	8
Conformité réglementaire .....	8
Architecture & infrastructure des données .....	11
Qualité des données .....	13
Mesures correctives de Facebook .....	15
Utiliser les <i>Normes</i> pour auditer l'intelligence artificielle .....	16
Conclusion .....	16

### Comité consultatif

Nur Hayati Baharuddin, CIA, CCSA, CFSA, CGAP, CRMA – IIA–Malaisie

Lesedi Lesetedi, CIA, QIAL – *African Federation IIA*

Hans Nieuwlands, CIA, CCSA, CGAP – IIA–Pays-Bas

Karem Obeid, CIA, CCSA, CRMA – IIA–Emirats Arabes Unis

Carolyn Saint, CIA, CRMA, CPA – IIA – Amérique du Nord

Ana Cristina Zambrano Preciado, CIA, CCSA, CRMA – IIA-Colombie

### Numéros précédents

Pour accéder aux numéros précédents de Perspectives Internationales, visitez le site à l'adresse suivante [www.theiia.org/gpi](http://www.theiia.org/gpi).

### Commentaires des lecteurs

N'hésitez pas à nous faire parvenir vos questions et vos commentaires à l'adresse suivante : [globalperspectives@theiia.org](mailto:globalperspectives@theiia.org)

Remarque : Il s'agit du deuxième volet d'une série en trois parties. Pour plus d'informations, consultez le premier volet : [Intelligence artificielle – Considérations pour la profession d'audit](#)

## Introduction

Un nouveau projet de Google nommé AutoML s'apprête à faire entrer l'intelligence artificielle - terme général qui désigne les technologies rendant les machines « intelligentes » - dans une nouvelle phase. ML, abréviation de *Machine Learning* (apprentissage automatique), se réfère aux algorithmes informatiques qui analysent des données pour apprendre à réaliser des tâches. AutoML est un algorithme d'apprentissage automatique qui apprend à développer d'autres algorithmes d'apprentissage automatique.

Jeff Dean, ingénieur chez Google, décrit le projet comme un moyen pour les entreprises de construire des systèmes à l'aide de l'intelligence artificielle, même si elles ne disposent pas d'une grande expertise en la matière. Selon lui, aujourd'hui seules quelques milliers d'entreprises possèdent les compétences adéquates pour développer l'intelligence artificielle, mais beaucoup plus disposent des données nécessaires. « *Nous voulons que les milliers d'entreprises capables de résoudre des problèmes d'apprentissage automatique deviennent des millions* », a-t-il déclaré au *New York Times*.

Google fait partie des nombreuses organisations qui investissent dans la recherche sur l'intelligence artificielle et ses applications pour automatiser, accroître ou reproduire l'intelligence humaine, c'est-à-dire les compétences analytiques et/ou la prise de décisions humaines. Suivant le mouvement de création initié par les sciences informatiques, Microsoft a récemment dévoilé un outil pour aider les codeurs à construire des « réseaux neuronaux profonds », une sorte d'algorithme informatique qui élimine « une grande partie des tâches difficiles », selon les déclarations de Joseph Sirosh, vice-président de Microsoft, au *Times*. Les efforts visant à encourager les initiatives des organisations en matière d'intelligence artificielle accentuent la nécessité pour la profession d'audit interne de bien se préparer à l'arrivée de cette dernière.

Outre l'apprentissage automatique, il existe de nombreux concepts associés à l'intelligence artificielle comme, par exemple, l'apprentissage profond, la reconnaissance d'image, le traitement du langage naturel, l'informatique cognitive, l'amplification de l'intelligence, l'augmentation cognitive, l'intelligence augmentée grâce aux machines et l'intelligence augmentée. L'intelligence artificielle, telle qu'elle est envisagée dans le Cadre de référence IIA pour l'audit de l'intelligence artificielle (Cadre de référence), englobe l'ensemble de ces concepts.

## Le cadre de référence IIA pour l'audit de l'intelligence artificielle

Comme expliqué dans le rapport Intelligence artificielle – Considérations pour la profession de l'audit interne, le rôle de l'audit interne est « *d'aider une organisation à évaluer, comprendre et communiquer la mesure dans laquelle l'intelligence artificielle aura un effet (négatif ou positif) sur la capacité de cette organisation à créer de la valeur à court, moyen, ou à long terme* ».

Pour remplir cette mission, les auditeurs internes peuvent tirer profit du Cadre de référence IIA pour l'audit de l'intelligence artificielle pour fournir des services de conseil ou d'assurance en lien avec l'intelligence artificielle, ou les deux en



fonction de l'organisation. Le Cadre de référence est constitué de trois composantes fondamentales, à savoir la stratégie relative à l'intelligence artificielle, la gouvernance et le facteur humain, et de sept sous-éléments : la cyber résilience, les compétences en intelligence artificielle, la qualité des données, l'architecture et l'infrastructure des données, la mesure de la performance, l'éthique et la boîte noire.

L'audit interne est tenu de considérer les nombreux objectifs de mission ou de contrôle ainsi que les activités ou procédures lors de la mise en œuvre du Cadre de référence et lors de la prestation de services de conseil, d'assurance, ou les deux, en lien avec les activités d'intelligence artificielle de l'organisation. Les objectifs et les activités ou procédures pertinents pour les volets stratégie (cyber résilience et compétences en intelligence artificielle) et gouvernance (architecture et infrastructure des données, qualité des données) du Cadre de référence sont fournis dans ce document. L'élément mesure de la performance et le volet facteur humain (éthique et boîte noire) seront abordés dans la partie III de cette série en trois volumes.

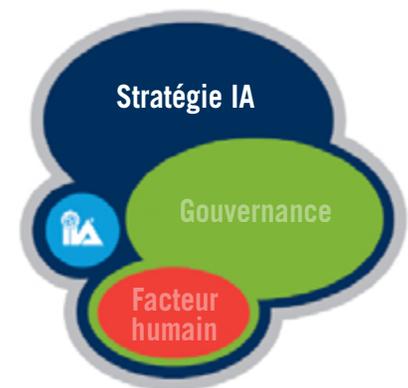
## Stratégie relative à l'intelligence artificielle

La stratégie en intelligence artificielle sera spécifique à chaque organisation et fondée sur son approche visant à tirer parti des opportunités qu'offre la technologie. Elle peut être une extension évidente de sa stratégie numérique globale ou de sa stratégie de *Big Data* et doit définir clairement les résultats attendus. Elle doit être développée conjointement par les dirigeants opérationnels, qui peuvent formuler ces résultats et la manière dont ces derniers concourent à l'atteinte des objectifs de l'organisation, et par les responsables SI qui comprennent les compétences, les contraintes et les aspirations technologiques de l'organisation en matière d'intelligence artificielle. Les dirigeants opérationnels et les techniciens doivent également être impliqués dans la mise en œuvre de cette stratégie.

L'intelligence artificielle dépend du *Big Data*. Par conséquent, une organisation doit pleinement développer et mettre en œuvre sa stratégie de *Big Data* avant d'envisager l'intelligence artificielle. En effet, cette dernière peut aider les organisations à mieux appréhender le *Big Data*. Comme décrit dans le GTAG « comprendre et auditer le *Big Data* » de l'IIA, « *en partant des nouvelles perspectives offertes par le Big Data, les organisations peuvent améliorer les processus de prise de décision, cibler de nouveaux clients de manière innovante et segmentée, servir les clients existants en adoptant un modèle de prestation amélioré et adapté à chacun, et offrir de nouveaux services et de nouvelles facilités permettant de se distinguer véritablement des concurrents.* » Les organisations qui tirent profit des opportunités offertes par le *Big Data* sont en mesure de développer un avantage concurrentiel durable et la stratégie en matière d'intelligence artificielle doit être développée et mise en œuvre dans le cadre de la cyber résilience et des compétences en intelligence artificielle.

### Cyber résilience

La capacité de l'organisation à résister, à réagir et à surmonter les cyberattaques, dont l'utilisation abusive et intentionnelle des technologies d'intelligence artificielle d'une organisation à des fins malveillantes, devient de plus en plus importante (cf. les mesures correctives de Facebook page 15). Les responsables



Avant que l'audit interne ne se lance dans l'évaluation de la stratégie relative à l'intelligence artificielle de l'organisation, il doit définir sa propre stratégie en la matière en l'incluant dans son évaluation des risques et en envisageant la possibilité de l'inclure dans le plan d'audit fondé sur les risques.

Les objectifs et les activités ou procédures pertinents identifiés par l'IIA ne comprennent pas un plan d'audit défini, mais constituent des exemples utiles pour identifier les objectifs de la mission ou du contrôle, et pour planifier et réaliser des missions d'audit dans le domaine de l'intelligence artificielle.

Ces dernières devraient respecter la Norme 2200 de l'IIA : Planification de la mission. Le plan d'audit et les objectifs et les procédures de la mission doivent toujours être adaptés pour répondre aux besoins de l'organisation.

de l'audit interne doivent rapidement acquérir des compétences en cybersécurité au sein de leur équipe, surveiller constamment les risques liés à l'intelligence artificielle / cybersécurité, et communiquer à la direction générale et au Conseil le niveau de risque encouru par l'organisation ainsi que les mesures à prendre pour y faire face.

## Compétences en intelligence artificielle

Comme indiqué dans Intelligence artificielle – Considérations pour la profession d'audit interne, le vivier de professionnels experts en intelligence artificielle est restreint. Même si des projets comme AutoML (cf. page 2) permettent aux organisations de construire des systèmes pourvus de l'intelligence artificielle alors qu'elles ne possèdent pas d'expertise propre, ces dernières devront tout de même combler leur déficit de connaissances en s'entourant de collaborateurs ayant une bonne compréhension de l'intelligence artificielle, même s'ils ne peuvent pas la « créer ». Ceux-ci doivent :

- savoir comment fonctionne l'intelligence artificielle ;
- comprendre les risques et les opportunités que l'intelligence artificielle représente ;
- déterminer si les résultats de l'intelligence artificielle correspondent aux attentes ;
- être capables de recommander ou de prendre des mesures correctives le cas échéant.

De telles compétences seront requises au niveau de l'audit interne et des première et deuxième lignes de maîtrise. La direction générale et le Conseil devraient également connaître le fonctionnement de l'intelligence artificielle et comprendre les risques et opportunités qu'elle représente.

De son côté, l'audit interne devrait être en mesure de déterminer si des prestataires extérieurs de technologies d'intelligence artificielle sont compétents.

## Objectifs et activités ou procédures pertinents pour la stratégie en intelligence artificielle

Objectif(s) de la mission ou du contrôle	Activités ou procédures
Être activement impliqué dès le début dans des projets relatifs à l'intelligence artificielle, donner des conseils et avis contribuant à la réussite de la mise en œuvre.	<b>Participer</b> aux réunions de l'équipe du projet d'intelligence artificielle.
L'organisation dispose d'une stratégie définie en intelligence artificielle.	<b>Déterminer</b> si une stratégie en intelligence artificielle a été documentée. Si oui, vérifier que la stratégie : <ul style="list-style-type: none"> <li>■ énonce les résultats escomptés des activités d'intelligence artificielle (objectifs stratégiques) ;</li> <li>■ définit à un niveau élevé la manière dont les objectifs en matière d'intelligence artificielle seront atteints (plan stratégique).</li> </ul>
Fournir une assurance concernant la réactivité et la réaction aux cybermenaces.	<b>Tirer profit</b> d'un cadre de cybersécurité établi, <b>travailler</b> en collaboration avec le département informatique et d'autres parties pour s'assurer que des défenses et des plans d'action efficaces sont en place.
Avoir suffisamment de ressources (collaborateurs et budget) pour mettre en œuvre la stratégie en intelligence artificielle.	<b>Analyser</b> le processus afin de définir les besoins en ressources humaines et financières pour développer et maintenir l'intelligence artificielle.
Déterminer si la stratégie prend suffisamment en compte les menaces et les opportunités de l'intelligence artificielle.	<b>Passer en revue</b> toutes les évaluations existantes portant sur les menaces et les opportunités de l'intelligence artificielle. Si aucune évaluation n'existe, <b>faire des recommandations</b> pour l'établir (comment l'organisation pourrait envisager d'identifier les menaces et les opportunités liées à l'intelligence artificielle).

## Gouvernance

La gouvernance de l'intelligence artificielle désigne les structures, les processus et les procédures mis en place pour diriger, gérer et surveiller les activités liées à l'intelligence artificielle au sein de l'organisation. La structure et la formalisation de la gouvernance dépendront des caractéristiques spécifiques à l'organisation. La gouvernance de l'intelligence artificielle :

- établit l'obligation de rendre compte, la responsabilité et la supervision ;
- contribue à garantir que les responsables de l'intelligence artificielle disposent des compétences et de l'expertise nécessaires ;
- contribue à garantir que les activités, les décisions et les actions relatives à l'intelligence artificielle respectent les valeurs ainsi que les responsabilités éthiques, sociales et légales de l'organisation.

Les règles et procédures en matière d'intelligence artificielle doivent être établies pour tout le cycle de vie de l'intelligence artificielle – des intrants aux extrants. Des règles et procédures doivent également être édictées pour la formation, la mesure de la performance et le *reporting*.



« Le cadre de référence IIA pour l'audit de l'intelligence artificielle est un outil pratique pour aider l'audit interne à fournir une assurance indépendante concernant les processus de management des risques, de contrôle et de gouvernance liés à l'intelligence artificielle ».

Nur Hayati Baharuddin,  
Membre, IIA-Malaisie

## Obligation de rendre compte, responsabilité et supervision

L'intelligence artificielle a le potentiel de faire beaucoup de bien et beaucoup de mal. Au bout du compte, les parties prenantes tiendront probablement le Conseil et la direction générale pour responsables des conséquences de l'utilisation de l'intelligence artificielle par leur organisation. Lors de l'évaluation de la gouvernance, les auditeurs internes peuvent avoir recours au modèle des trois lignes de maîtrise. Dans ce modèle, la direction générale, l'organe de gouvernance, les auditeurs externes et les régulateurs ont tous un rôle à jouer en matière d'intelligence artificielle. Les auditeurs internes doivent comprendre le rôle de chaque partie et comment interagir avec chacune.

### Régulateurs

Les régulateurs informent et contrôlent des secteurs spécifiques (comme la banque, les soins de santé ou la sécurité alimentaire) aux niveaux national, régional et local. Ils « informent » par le biais d'activités telles que la recherche, la participation à l'élaboration de normes et lignes directrices et la communication avec les parties prenantes, et « contrôlent » par le biais d'activités comme la supervision, l'établissement et la mise en vigueur de réglementations. Comme indiqué dans la prise de position de l'IIA : [Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces](#), il arrive parfois que les régulateurs aient des exigences visant à renforcer les contrôles au sein des organisations et procèdent ponctuellement à des revues indépendantes et objectives afin d'évaluer en tout ou partie les première, deuxième ou troisième lignes de maîtrise à l'aune de ces exigences.

A ce jour, il n'existe aucune réglementation dédiée exclusivement à l'intelligence artificielle. Toutefois, certaines parties de réglementations existantes peuvent être pertinentes pour les activités d'intelligence artificielle. Les régulateurs et les organismes de normalisation du monde entier ont fait part de leurs inquiétudes au travers des recherches conduites, de documents de réflexion, de recommandations et de lignes directrices (cf. Conformité réglementaire page 7).

Les régulateurs reconnaissent déjà l'importance des missions d'audit relatives à l'intelligence artificielle. Par exemple, dans son document [Off-The-Shelf Software Use in Medical Devices](#), la *Food and Drug Administration* (FDA) reconnaît l'importance d'auditer les logiciels prêts à l'emploi fondés sur la connaissance (ex : un logiciel d'intelligence artificielle, de systèmes experts ou de réseau neuronal), soulignant que le fabricant doit fournir l'assurance « *que les méthodes de développement du produit, utilisées par le développeur du logiciel prêt à l'emploi, sont adéquates et suffisantes pour l'usage prévu...* ». En outre, la FDA « *recommande que cette assurance inclut un audit des méthodologies de conception et de développement du développeur du logiciel prêt à l'emploi, utilisées dans la création dudit logiciel. Cet audit doit évaluer de manière approfondie les documents de développement et de qualification générés pour le logiciel prêt à l'emploi* ».

Les auditeurs devraient se tenir informés du travail des régulateurs et des normalisateurs dans le domaine de l'intelligence artificielle, prévenir la direction et le Conseil des questions d'importance et évaluer si les objectifs de l'organisation en termes de contrôle réglementaire tiennent compte des réglementations, des normes et des lignes directrices émergentes.

## Organe de gouvernance / Conseil / Comité d'audit

Le Conseil est responsable en dernier ressort de la supervision des activités d'intelligence artificielle de l'organisation. Il devrait s'associer à la direction générale pour définir la stratégie en intelligence artificielle de l'organisation.

L'audit interne doit comprendre et être bien informé de ce qu'est l'intelligence artificielle en général et, plus particulièrement des activités de l'organisation en la matière. En outre, afin de fournir une assurance sur les activités d'intelligence artificielle, l'audit interne devrait proposer des conseils et points de vue pour veiller à ce que le Conseil soit préparé pour son rôle.

## Direction générale

En collaboration avec le Conseil, la direction générale définit la stratégie relative à l'intelligence artificielle de l'organisation, ainsi que les objectifs en lien avec l'intelligence artificielle et met en place des plans de mise en œuvre de cette stratégie.

L'audit interne devrait être représenté au sein de l'équipe de direction et tenu au courant des initiatives de la direction générale en matière d'intelligence artificielle. Concernant les processus de management des risques, de gouvernance et de contrôle relatifs à l'intelligence artificielle, l'audit interne devrait faire office de conseiller de confiance auprès de la direction générale.

## Première ligne de maîtrise

Les managers opérationnels devraient s'appropriier et gérer les risques relatifs à l'intelligence artificielle au quotidien. L'audit interne devrait évaluer les règles et procédures en matière d'intelligence artificielle au niveau des opérations, en vérifiant que les objectifs de contrôle sont adaptés et mis en œuvre comme prévu.

## Deuxième ligne de maîtrise

La conformité, l'éthique, le management des risques et la confidentialité/sécurité des informations constituent certaines fonctions de la deuxième ligne de maîtrise qui auront probablement un rôle à jouer dans certains aspects des risques de l'intelligence artificielle. L'audit interne devrait évaluer les règles et procédures définies par la deuxième ligne de maîtrise dans le domaine de l'intelligence artificielle, en vérifiant que les objectifs de contrôle sont adaptés et mis en œuvre comme prévu.

## Troisième ligne de maîtrise

L'audit interne devrait fournir une assurance indépendante sur les risques, la gouvernance et les dispositifs de contrôle associés à l'intelligence artificielle. Le Cadre de référence IIA pour l'audit de l'intelligence artificielle peut lui faciliter la tâche. Les régulateurs et normalisateurs ont reconnu le potentiel de l'intelligence artificielle dans le management des risques et la conformité. Selon le rapport du *Financial Stabilities Board* (FSB) sur l'intelligence artificielle dans la finance (*Artificial intelligence and machine learning in financial services*), « le recours à l'intelligence artificielle et à l'apprentissage automatique dans les services financiers peut offrir des avantages clés en termes de stabilité financière, notamment des gains d'efficacité au niveau de la prestation de services financiers et de la surveillance des risques systémiques réglementaires... Les applications

« En plus de fournir une assurance sur les activités d'intelligence artificielle, l'audit interne doit veiller à ce que les comités d'audit et les Conseils soient à même de comprendre leur rôle dans la gestion des bénéfices et des risques associés à l'intelligence artificielle dans leurs organisations ».

Carolyn Saint, responsable de  
l'audit interne, University of  
Virginia

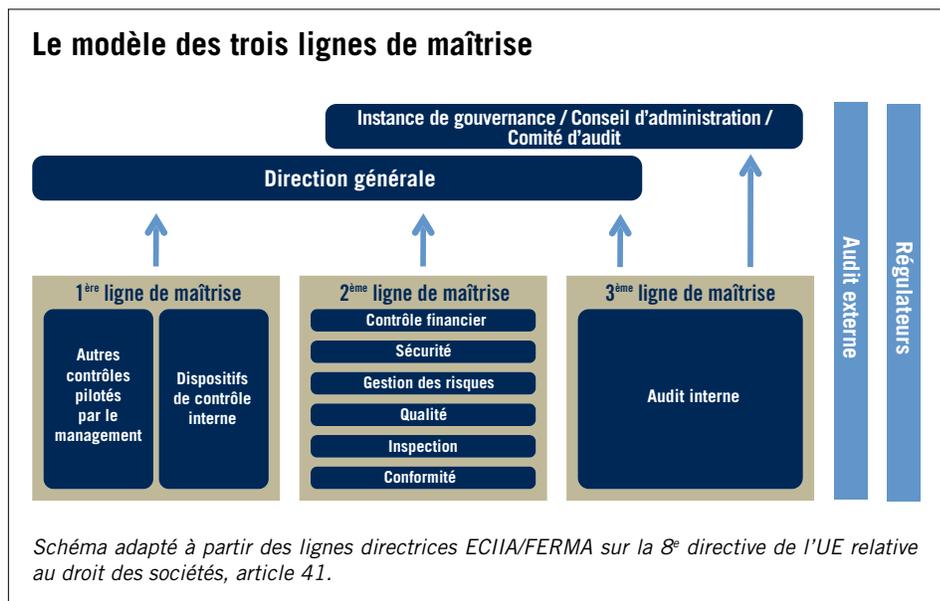
« L’usage émergent de l’intelligence artificielle requiert de l’audit qu’il s’attarde spécifiquement sur la logique utilisée pour concevoir les algorithmes ».

Hans Nieuwlands, directeur général, IIA–Pays-Bas

*internes (back office) de l’intelligence artificielle et de l’apprentissage automatique pourraient améliorer le management des risques, la détection des fraudes et la conformité avec les exigences réglementaires, potentiellement à moindre coût* ». De la même manière, les fonctions d’audit interne les plus avancées commenceront à utiliser les algorithmes pour alimenter leurs initiatives d’audit et de contrôle en continu, gagnant ainsi en efficacité et en efficience.

### Audit externe

Les auditeurs externes sont des tiers n’ayant aucun intérêt direct dans l’organisation. Ils donnent un avis sur les états financiers, afin de déterminer s’ils ont été préparés conformément aux cadres de l’information financière et/ou aux réglementations applicables. Concernant l’intelligence artificielle, les auditeurs externes vont plutôt se concentrer sur les résultats, par exemple, sur les algorithmes derrière le modèle en matière de gestion ou d’évaluation des risques, ou déterminer si ces algorithmes ont un impact matériel sur les états financiers de l’organisation.



### Conformité réglementaire

De manière générale, la réglementation est en retard sur le changement technologique, et le cas de l’intelligence artificielle ne déroge pas à la règle. Cependant, comme rapporté par [The Hill](#), le directeur général de Tesla, Elon Musk, a mis en garde la *National Governors Association* (États-Unis) sur la nécessité d’établir des réglementations au plus vite. En outre, les réglementations relatives à la protection de la vie privée, telles que la loi américaine *Health Insurance Portability and Accountability Act* (HIPAA) de 1996 et le Règlement Général sur la Protection des Données (RGPD) de l’UE, qui entrera en vigueur en mai 2018, risquent de compliquer la mise en œuvre de l’intelligence artificielle. Ces deux règlements protègent les données à caractère personnel qui sont généralement les données entrantes des technologies d’intelligence artificielle.

Par exemple, la [loi HIPAA](#) « définit des normes nationales relatives à la protection des données médicales qui s'appliquent aux trois types d'entités couvertes, à savoir les plans de santé, les bureaux de compensation des soins de santé et les prestataires de soins de santé qui exécutent certaines transactions médicales par voie électronique ». Et selon le rapport du *Financial Stabilities Board* (FSB) sur l'intelligence artificielle dans la finance, « plusieurs sections du RGPD sont particulièrement pertinentes pour l'intelligence artificielle: l'article 11 octroie "le droit d'obtenir une explication quant à la décision prise à l'issue de l'évaluation" ». L'article 9 interdit le traitement de « catégories particulières de données à caractère personnel (sensibles) ». L'article 22 stipule que la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative. Enfin, l'article 24 indique que les décisions ne peuvent être fondées sur les catégories particulières de données à caractère personnel.

Parmi d'autres préoccupations réglementaires connues, on retrouve la conformité avec les lois anti-discrimination et les obligations juridiques, particulièrement vis-à-vis de tiers qui fournissent des services d'intelligence artificielle à l'organisation. Le FSB a résumé ces dernières en déclarant : « La plupart des prestataires de services d'intelligence artificielle et d'apprentissage automatique dans le secteur de la finance peuvent se situer en dehors du périmètre réglementaire ou ne pas connaître les lois et les réglementations en vigueur. Lorsque des établissements financiers dépendent de prestataires extérieurs pour des services d'intelligence artificielle et d'apprentissage automatique destinés à des fonctions essentielles, et que les règles de sous-traitance sont inexistantes ou incomprises, il est possible que ces prestataires ne soient pas sujets à une quelconque supervision. De la même manière, si les prestataires de ces outils se mettent à proposer des services financiers à leurs clients institutionnels ou de détail, cela pourrait entraîner une exclusion des activités financières du périmètre réglementaire ».

Les organisations ne devraient pas attendre que le cadre réglementaire rattrape son retard sur les technologies. Même si les réglementations existantes ne ciblent pas spécifiquement l'intelligence artificielle, la *lettre* de la loi, les organisations doivent vérifier que leurs activités d'intelligence artificielle sont en accord avec l'*esprit* des lois existantes. Une approche envisageable consiste à réaliser des scénarios et des analyses d'hypothèses afin de définir si les activités en matière d'intelligence artificielle peuvent potentiellement servir à des fins malveillantes ou criminelles, ou avoir des conséquences imprévues causant des dommages. Les responsables de la gouvernance doivent également envisager que les activités d'intelligence artificielle puissent éventuellement affaiblir les dispositifs de contrôle interne si l'intelligence artificielle apprend à contourner les règles établies ou si les systèmes d'intelligence artificielle apprennent à communiquer les uns avec les autres et à « coopérer » à l'insu de l'organisation. Une approche proactive considérant l'esprit des lois existantes aidera les organisations à être flexibles lorsque de nouvelles réglementations seront promulguées et entreront en vigueur.

## Objectifs et activités ou procédures pertinents pour la gouvernance de l'intelligence artificielle

### Objectif(s) de la mission ou du contrôle

### Activités ou procédures

**Fournir l'assurance** que les structures de gouvernance de l'intelligence artificielle ont été établies, documentées et fonctionnent comme prévu.

**Examiner** les modèles économiques et la structure organisationnelle; **déterminer** si ces derniers reflètent la stratégie en intelligence artificielle de l'organisation.

**Examiner** les règles et procédures en matière d'intelligence artificielle; **déterminer** si celles-ci identifient clairement les rôles et responsabilités liés à la stratégie, à la gouvernance, à l'architecture des données, à la qualité des données, aux exigences éthiques et à la mesure de la performance en matière d'intelligence artificielle.

**Évaluer** si les responsables de l'intelligence artificielle disposent des compétences requises pour être performants. Par exemple, les responsables Éthique doivent pouvoir évaluer le comportement éthique de ceux qui alimentent l'intelligence artificielle d'inputs humains, et devraient être indépendants de l'activité d'intelligence artificielle.

**S'entretenir** avec les responsables de l'intelligence artificielle.

**Passer en revue** les descriptions des postes liés à l'intelligence artificielle, les compétences requises etc., et **vérifier** que les responsables disposent bien des qualifications annoncées.

**Fournir l'assurance** que les règles et procédures en matière d'intelligence artificielle ont été établies et documentées.

**Examiner** les règles et procédures en matière d'intelligence artificielle et **déterminer** si elles traitent correctement les risques relatifs à l'intelligence artificielle.

**Déterminer** si les règles et procédures permettent de réaliser régulièrement des analyses d'hypothèses et d'élaborer des scénarios.

**Fournir l'assurance** que les pistes d'audit de l'activité d'intelligence artificielle donnent suffisamment d'informations pour comprendre quelles décisions ont été prises et pourquoi.

**Examiner** toutes les pistes d'audit de l'activité d'intelligence artificielle.

**Déterminer** si les pistes d'audit donnent suffisamment d'informations pour comprendre quelles décisions ont été prises et pourquoi.

**Fournir l'assurance** que les règles et procédures ont été mises en œuvre et fonctionnent comme prévu, et que les collaborateurs les respectent.

**Observer** les collaborateurs appliquer les procédures en matière d'intelligence artificielle.

**Examiner** les rapports des services d'assistance et **assurer un suivi** de tous les rapports contenant des allégations des activités non-conformes ou malveillantes en lien avec l'intelligence artificielle.

**S'entretenir** avec un échantillon aléatoire de collaborateurs et déterminer s'ils ont connaissance des règles et procédures en matière d'intelligence artificielle.

**Identifier** et **examiner** les règles et procédures d'accès à l'intelligence artificielle.

**Évaluer** les politiques d'accès et **tester** les contrôles d'accès.

**Évaluer** si les objectifs de contrôle réglementaire tiennent compte des réglementations, des normes et des lignes directrices émergentes.

## Architecture & infrastructure des données

De même que pour le traitement du *Big Data*, l'architecture et l'infrastructure des données de l'intelligence artificielle seront probablement combinées. Les pistes suivantes doivent être étudiées :

- La manière dont les données sont accessibles (métadonnées, taxonomie, identificateurs uniques et conventions de nommage).
- La confidentialité et la sécurité des informations tout au long du cycle de vie des données (collecte, utilisation, stockage et destruction des données).
- Les rôles et les responsabilités en matière de propriété des données et de leur utilisation tout au long du cycle de vie des données.

Selon [InfoWorld](#), les organisations devraient porter leur attention sur trois aspects majeurs du développement de logiciel pour garantir une bonne intégration de l'intelligence artificielle :

- L'intégration des données – les données issues de sources multiples doivent être intégrées avant d'incorporer l'intelligence artificielle dans les applications et systèmes de l'organisation.
- La modernisation des applications – des mises à jour logicielles périodiques sont requises. On préfère des mises à jour fréquentes, moins lourdes aux mises à jour intensives plus ponctuelles qui ralentissent ou perturbent les systèmes.
- La formation des collaborateurs – les développeurs de logiciel, les chefs de projets et les autres collaborateurs en charge des technologies doivent se tenir informés des avancées en matière d'apprentissage automatique et de chaque aspect du socle technologique (logiciels et composants nécessaires au fonctionnement de l'intelligence artificielle).

En outre, les données doivent être rapprochées afin que des nuances comme les arrondis, les données démographiques et d'autres variables soient normalisées avant d'être injectées.

« L'architecture & infrastructure des données et la qualité des données sont souvent entremêlées. Les objectifs de la mission ou du contrôle et les activités et procédures pertinents dans un domaine peuvent se chevaucher ou avoir un impact sur les objectifs, activités et procédures d'un autre domaine ».

Lesedi Lesetedi,  
Directeur général adjoint  
– Stratégie & Services aux  
entreprises  
Botswana College of Distance &  
Open Learning (BOCODOL)

## Objectifs et activités ou procédures pertinents pour l'architecture et l'infrastructure des données

### Objectif(s) de la mission ou du contrôle

**Fournir une assurance** sur la cyber résilience de l'organisation. La cyber résilience ne se limite pas à la cybersécurité. Elle englobe la sécurité (résistance), la réponse et la reprise d'activité.

**Fournir l'assurance** que l'infrastructure des données a la capacité de s'adapter à la taille et à la complexité des activités d'intelligence artificielle définies dans la stratégie.

**Fournir l'assurance** que l'organisation a établi une taxonomie des données. Évaluer la qualité, l'exhaustivité et la cohérence de l'usage de la taxonomie des données au niveau de l'entreprise.

### Activités ou procédures

**Comprendre et auditer** le *Big Data* (cf. le Guide pratique de l'IIA : comprendre et auditer le *Big Data*).

**Évaluer** si l'organisation se prépare à se conformer aux nouvelles réglementations en matière de technologies, telles que le Règlement Général sur la Protection des Données (RGPD) de l'UE.

**Évaluer** si les plans de reprise après sinistre de l'organisation prennent en compte les défaillances de l'intelligence artificielle, et particulièrement des contrôles préservant les règles établies par la gouvernance de l'intelligence artificielle.

**Évaluer** si l'infrastructure est en mesure de traiter des données structurées et non-structurées.

**Évaluer** si la taxonomie est suffisamment robuste pour s'adapter à la taille et à la complexité des activités d'intelligence artificielle.

## Qualité des données

L'exhaustivité, la précision et la fiabilité des données sur lesquelles sont construits les algorithmes de l'intelligence artificielle sont essentielles. Pour que l'intelligence artificielle soit efficace, les organisations doivent accéder à de grandes quantités de données de haute qualité, c'est-à-dire des données bien définies et dans des formats normalisés. Souvent, les systèmes ne communiquent pas entre eux ou le font par le biais de modules complémentaires ou d'adaptations complexes. La manière dont ces données sont rapprochées, synthétisées et validées est cruciale afin que les systèmes qui ne communiquent pas entre eux ou qui le font au moyen de modules complémentaires ou d'adaptations complexes, ne puissent pas entraver les activités d'intelligence artificielle d'une organisation.

En marge des données bien définies et dans des formats normalisés (données structurées), les technologies d'intelligence artificielle peuvent dépendre de données non structurées (comme les posts sur les réseaux sociaux). Comme décrit dans le «GTAG: comprendre et auditer le *Big Data*» de l'IIA, des données non structurées sont *«généralement plus difficiles à gérer, en raison de leur nature évolutive et imprévisible, mais aussi en raison du nombre et de la diversité de leurs sources souvent externes. Par conséquent, de nouvelles solutions ont été développées pour gérer et analyser ce type de données»*.

Paradoxalement, les organisations peuvent recourir à l'apprentissage automatique – une forme d'intelligence artificielle – pour améliorer la qualité des données. Par exemple, il peut y avoir de nombreuses versions du nom d'un vendeur dans les multiples unités opérationnelles, bases de données et tableurs d'une organisation. Un programme informatique pourrait scanner et rapprocher toutes les variations du nom en quelques heures ou quelques minutes.

L'audit interne devrait également analyser comment les données utilisées dans les rapports d'audit interne ont été rapprochées, synthétisées et validées.

## Objectifs et activités ou procédures pertinents pour la qualité des données

### Objectif(s) de la mission ou du contrôle

**Fournir une assurance** sur la fiabilité des algorithmes sous-tendant l'intelligence artificielle, ainsi que les données sur lesquelles ces derniers s'appuient.

**Fournir l'assurance** que les données entrantes sont rapprochées et normalisées pour une précision optimale.

**Fournir l'assurance** que les données agrégées sont complètes.

**Fournir l'assurance** que l'exhaustivité des données est mesurée et contrôlée et que toute exception notable ayant une influence sur la prise de décision, est identifiée et expliquée. Cela devrait être systématique, que les exceptions soient humaines ou découlent de l'intelligence artificielle.

### Activités ou procédures

**Obtenir** un échantillon de données brutes qui alimentent l'intelligence artificielle.

**Vérifier** que l'organisation a mis en place des méthodologies dans le but de valider les résultats de l'intelligence artificielle en les comparant aux résultats du monde « réel », et qu'il existe des règles et procédures pour mesurer, surveiller, communiquer et rectifier en permanence des incohérences entre les deux.

**Vérifier** que l'organisation dispose de règles et procédures pour mesurer, surveiller, communiquer et résoudre les problèmes relevant de la précision et de l'intégrité des données.

**Confirmer** que l'organisation suit et surveille en continu un cadre formalisé de rapprochement des données, qui comprend une logique pour différencier les méthodologies des résultats, s'ils existent.

**Vérifier** que l'organisation dispose de règles et procédures pour limiter les biais pouvant altérer les données en entrée.

**Examiner** les mesures et rapports de mesure de l'intelligence artificielle.

**Évaluer** si les décideurs ont reçu et tenu compte des explications sur les exceptions notables associées à la qualité des données.

## Mesures correctives de Facebook

Les difficultés rencontrées par Facebook en matière d'intelligence artificielle ont fait grand bruit. Le géant des réseaux sociaux a fait l'objet d'une enquête sur la manière dont des technologies algorithmiques ont été utilisées – ou mal utilisées – à des fins malveillantes.

### Chronologie des faits marquants :

- À l'automne 2016, ProPublica a rapporté que les annonceurs pourraient utiliser les outils de ciblage publicitaire de Facebook pour exclure certaines races, ce qui représenterait une violation potentielle des réglementations fédérales en matière de droits au logement et de droits civils.
- En septembre 2017 :
  - o Facebook a révélé que des détenteurs de faux comptes basés en Russie avaient acheté de nombreux espaces publicitaires mettant en avant des sujets controversés en vue de l'élection présidentielle américaine de 2016.
  - o ProPublica a rapporté que les outils de ciblage publicitaire de Facebook ont permis aux annonceurs de cibler des racistes autoproclamés.
- En octobre 2017, des inquiétudes quant à la propagation de fausses informations ont refait surface lorsque Facebook (et Google) ont diffusé des informations erronées sur la fusillade de Las Vegas.
- Lors de son audition à la sous-commission judiciaire du Sénat américain fin octobre, Facebook a déclaré que la portée des publicités financées par la Russie s'étendait bien au-delà de ce qu'ils pensaient au départ, atteignant 126 millions d'Américains avant et pendant l'élection présidentielle de 2016.

### Réponse de Facebook

Dans un [post](#) du 20 septembre 2017, Sheryl Sandberg, directrice des opérations de Facebook, a annoncé trois mesures correctives :

1. Facebook est en train de clarifier ses politiques publicitaires et de resserrer ses processus d'exécution afin de s'assurer que les contenus qui vont à l'encontre des normes de la communauté de Facebook ne puissent pas être utilisés pour faire de la publicité ciblée. (Les politiques et processus relèvent de la composante Gouvernance du Cadre de référence. La gouvernance de l'intelligence artificielle doit notamment établir la responsabilité et la supervision de l'exécution des politiques.)
2. Facebook renforce « les contrôles et la surveillance d'origine humaine » de ses processus automatisés. (Les contrôles et la surveillance d'origine humaine ont trait à la composante Éthique du Cadre de référence. L'éthique détermine notamment si les résultats de l'intelligence artificielle tiennent compte des objectifs initiaux et s'ils sont utilisés de manière légale, éthique et responsable.)
3. Facebook élabore un programme pour encourager ses utilisateurs à signaler des abus potentiels de son système publicitaire. (Les systèmes de reporting se rapportent à la composante Mesure de la performance du Cadre de référence. Les systèmes de reporting aident le management à contrôler la performance des activités d'intelligence artificielle. La mesure de la performance sera couverte dans un prochain rapport de Perspectives internationales.)

En utilisant le Cadre de référence IIA pour l'audit de l'intelligence artificielle, les auditeurs internes peuvent fournir des services d'assurance et de conseil afin d'aider les organisations à distinguer la fiction et la réalité, et à gérer les risques liés au reporting, aux opérations et à la conformité associés à l'intelligence artificielle.

## Point d'attention

### Principales normes de l'IIA

Les *Normes internationales pour la pratique professionnelle de l'audit interne* de l'IIA comprennent plusieurs normes qui sont particulièrement pertinentes pour l'intelligence artificielle, dont :

Norme de l'IIA 1210 :  
compétence

Norme de l'IIA 2010 :  
planification

Norme de l'IIA 2030 : gestion des  
ressources

Norme de l'IIA 2100 : nature du  
travail

Norme de l'IIA 2110 :  
gouvernance

Norme de l'IIA 2130 : contrôle

Norme de l'IIA 2200 :  
planification de la mission

Norme de l'IIA 2201 :  
considérations relatives à la  
planification

Norme de l'IIA 2210 : objectifs  
de la mission

Norme de l'IIA 2220 : périmètre  
d'intervention de la mission

Norme de l'IIA 2230 : ressources  
affectées à la mission

Norme de l'IIA 2240 : programme  
de travail de la mission

Norme de l'IIA 2310 :  
identification des informations

## Utiliser les *Normes* pour auditer l'intelligence artificielle

Lors de la planification et la réalisation de missions liées à l'intelligence artificielle, les auditeurs internes devraient se conformer à toutes les normes applicables de l'IIA. Les principales normes de l'IIA, particulièrement pertinentes pour l'intelligence artificielle, sont reprises dans l'encadré ci-contre, mais d'autres peuvent également s'appliquer.

Chaque Norme est complétée par un Guide de mise en œuvre. Ces guides accompagnent les auditeurs internes dans l'application des *Normes*. Ensemble, ils abordent l'approche, les méthodologies et les considérations de l'audit interne, mais ne détaillent pas les processus et procédures.

## Conclusion

Le Cadre de référence IIA pour l'audit de l'intelligence artificielle permettra aux auditeurs internes d'aborder les services de conseil et d'assurance relatifs à l'intelligence artificielle, de manière systématique et disciplinée. Que les technologies et activités d'intelligence artificielle de l'organisation soient développées en interne, par le biais d'outils comme AutoML ou par un tiers, l'audit interne devrait être préparé à épauler le Conseil et la direction générale, à se coordonner avec les première et la deuxième lignes de maîtrise et à fournir une assurance sur les dispositifs de management des risques, de gouvernance et de contrôle associés à l'intelligence artificielle.

Ce rapport est la Partie II d'une série en trois volumes. Il propose des suggestions pour la mise en œuvre des composantes Stratégie relative à l'intelligence artificielle et Gouvernance du Cadre de référence IIA pour l'audit de l'intelligence artificielle. La partie III fera d'autres suggestions pour la mise en œuvre de la composante Gouvernance et du volet Facteur humain.

### À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'*Institute of Internal Auditors* (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires.

Son siège se situe à Lake Mary (Floride) aux États-Unis. Plus d'informations sont disponibles sur le site [www.globaliia.org](http://www.globaliia.org) ou [www.theiia.org](http://www.theiia.org)

### Clause de non-responsabilité

Les opinions exprimées dans les Perspectives internationales ne sont pas nécessairement celles des auteurs ayant collaboré à l'élaboration du présent document ni celles des collaborateurs.

### Copyright

Copyright © 2017 de l'Institute of Internal Auditors, Inc. Tous droits réservés.

